EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S18	162	(SAK SAS security adj (attention memory)) same (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 15:53
S19	6	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) same (SAK SAS security adj (attention memory)) same (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 15:57
S20	261	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) same (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 17:38
S21	71	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near7 (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 16:21
S22	748	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) and "726"/$.ccls. not S21	US-PGPUB; USPAT	OR	OFF	2006/04/03 16:23
S23	1	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1)) near20 authenticat$ and "726"/$.ccls. not S21	US-PGPUB; USPAT	OR	OFF	2006/04/03 16:24
S24	33	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1)) same authenticat$ and "726"/$.ccls. not S21	US-PGPUB; USPAT	OR	OFF	2006/04/03 17:38
S25	13	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1)) near25 authenticat$	EPO; JPO; DERWENT	OR	OFF	2006/04/03 16:29
S26	57173	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near5 (program$1 task$1 application$1 routine$1 processes$1)) not l8near25 authenticat$	EPO; JPO; DERWENT	OR	OFF	2006/04/03 16:29

EAST Search History

S27	6	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near5 (program$1 task$1 application$1 routine$1 processes$1)) near25 authenticat$ not S25	EPO; JPO; DERWENT	OR	OFF	2006/04/03 16:29
S28	19	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near5 (program$1 task$1 application$1 routine$1 processes$1)) same authenticat$ and "726"/$.ccls. not (S21 S24)	US-PGPUB; USPAT	OR	OFF	2006/04/03 16:30
S29	71	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near7 (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/05 15:53
S30	208	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) same (authenticat$3)not S29	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:12
S31	90	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near15 (password)not S29	US-PGPUB; USPAT	OR	OFF	2006/04/03 17:39
S32	88	S31 not (S30 S29)	US-PGPUB; USPAT	OR	OFF	2006/04/03 17:51
S33	351	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) and (authenticat$3).ab.	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:12
S34	261	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) same (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:13
S35	71	(halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near7 (authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:13
S36	208	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) same (authenticat$3)not S35	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:13

EAST Search History

S37	90	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near15 (password)not S35	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:30
S38	228	S33 not (S34 S35 S37 S36 "s88")	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:13
S39	57	(halt$ stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near15 (password)not S35	US-PGPUB; USPAT	OR	OFF	2006/04/03 20:13
S40	0	(sav$3 near4 state)near5 (program$1 task$1 application$1 routine$1 processes$1) same (interrupt and authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/05 15:54
S41	14	(state)near5 (program$1 task$1 application$1 routine$1 processes$1) same (interrupt and authenticat$3)	US-PGPUB; USPAT	OR	OFF	2006/04/05 15:56
S42	1	"5652890".pn. and inter$	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:23
S43	0	"5652890".pn. and authent$5	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:27
S45	12	(halt$ paus$ stop$ frozen freez$ imped$ delay$)and "5652890"	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:28
S46	1	(halt$ paus$ stop$ frozen freez$ imped$ delay$) and "5652890".pn.	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:29
S47	8	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near15 (secure adj mode)	US-PGPUB; USPAT	OR	OFF	2006/04/05 16:31
S48	1	(halt$ disabl$4 stop$3 ceas$3 paus$3 suspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1) near15 (secure adj mode)	EPO; JPO; DERWENT	OR	OFF	2006/04/05 16:38
S49	1	"20020066039" and screen$	EPO; JPO; DERWENT	OR	OFF	2006/04/05 16:38
S50	1	"20020066039" and screen$ and authenticat$	EPO; JPO; DERWENT	OR	OFF	2006/04/05 19:15
S51	0	(curtain atomic) near4 authenticat$3	EPO; JPO; DERWENT	OR	OFF	2006/04/05 19:16
S52	0	(curtain atomic) near4 authenticat$4	EPO; JPO; DERWENT	OR	OFF	2006/04/05 19:16

EAST Search History

S53	5	(curtain atomic) same authenticat$4	EPO; JPO; DERWENT	OR	OFF	2006/04/05 19:17
S54	20	(curtain atomic adj transaction$1) same authenticat$4	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:17
S55	31	(curtain$ atomic adj transaction$1) same authenticat$4	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:21
S56	13	(curtain$ atomic adj transaction$1) same authenticat$4 and ((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (code program$1 task$1 application$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:22
S57	8	(curtain$ atomic adj transaction$1) same authenticat$4 and ((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:23
S58	0	(curtain$ atomic adj transaction$1) same authenticat$4 and ((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5) near3 (program$1 task$1 application$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:22
S59	63289	((halt$ disabl$4 stop$3 ceas$3 paus$3 susspen$5 interrupt$3) near3 (program$1 task$1 application$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:24
S60	4905	((halt$ paus$3 susspen$5) near3 (program$1 task$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:24
S61	557	((halt$ paus$3 susspen$5) near3 (program$1 task$1 routine$1 processes$1)) same ((restart$3 start$3 restat$3)near3 (program$1 task$1 routine$1 processes$1))	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:25
S62	3	((halt$ paus$3 susspen$5) near3 (program$1 task$1 routine$1 processes$1)) same ((restart$3 start$3 restat$3)near3 (program$1 task$1 routine$1 processes$1)) same secur$3	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:27
S63	22	((halt$ paus$3 susspen$5) near3 (program$1 task$1 routine$1 processes$1)) same ((restart$3 start$3 restat$3)near3 (program$1 task$1 routine$1 processes$1)) and ((secur$3).ab. secur$3.ti.)	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:27

EAST Search History

S64	22	((halt$ paus$3 susspen$5) near3 (program$1 task$1 routine$1 processes$1)) same ((restart$3 start$3 restat$3)near3 (program$1 task$1 routine$1 processes$1)) and ((secur$3).ab. secur$3.ti.) not S62	US-PGPUB; USPAT	OR	OFF	2006/04/05 19:29

File 348:EUROPEAN PATENTS 1978-2006/ 200613
(c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060330,UT=20060323
(c) 2006 WIPO/Univentio

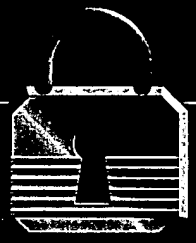
Set	Items	Description
S1	2769447	PROGRAM? ? OR APPLICATION? ? OR MODULE? ? OR ROUTINE? ? OR PROCESSES OR THREAD? ? OR TASK? ?
S2	566048	RUN OR RUNNING OR EXECUT???
S3	340172	MEMORY OR RAM
S4	29121	S1(7N)S2:S3(7N)(SUSPEND??? OR SUSPENSION OR DEFER??? OR DEFERMENT OR DELAY??? OR INHIBIT? OR HALT??? OR PREVENT??? OR DISABL? OR HINDER??? OR STOP???? OR BLOCK??? OR RESTRICT??? OR IMPED??? OR FREEZ??? OR FROZEN OR PAUS??? OR INTERRUPT?)
S5	236175	PIN OR PERSONAL()IDENTIFICATION()NUMBER? ? OR PASSWORD? ? OR PASSCODE? ? OR PASSPHRASE? ? OR (PASS OR SECRET)()(WORD? ? OR CODE? ? OR PHRASE? ?) OR CREDENTIAL? ? OR AUTHENTICAT?
S6	79650	S5(7N)(ENTER??? OR ENTRY OR INPUT??? OR SUBMIT? OR TYPE? ? OR TYPING OR PROVID??? OR SUPPLY??? OR SUPPLIES OR SUPPLIED OR WRIT??? OR PRESENT???)
S7	7684	S5(7N)(SCREEN? ? OR BOX? ? OR PROMPT???)
S8	346	S4(50N)S6:S7
S9	153	S4(50N)S6:S7(50N)(KEY? ? OR KEYBOARD? ? OR KEYPAD? ? OR CLICK??? OR PRESS?? OR PRESSING OR BUTTON? ?)
S10	77	S9 AND AC=US/PR AND AY=(1978:2000)/PR
S11	77	S9 AND AC=US AND AY=1978:2000
S12	77	S9 AND AC=US AND AY=(1978:2000)/PR
S13	76	S9 AND PY=1978:2000
S14	98	S10:S13
S15	98	IDPAT (sorted in duplicate/non-duplicate order)

```
File 347:JAPIO Nov 1976-2005/Nov(Updated 060302)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200622
         (c) 2006  Thomson Derwent

Set     Items   Description
S1    2025902   PROGRAM? ? OR APPLICATION? ? OR MODULE? ? OR ROUTINE? ? OR
               PROCESSES OR THREAD? ?
S2     883128   RUN OR RUNNING OR EXECUT???
S3    1044662   MEMORY OR RAM
S4      14932   S1(7N)S2:S3(7N)(SUSPEND??? OR SUSPENSION OR DEFER??? OR DE-
               FERMENT OR DELAY??? OR INHIBIT? OR HALT??? OR PREVENT??? OR D-
               ISABL? OR HINDER??? OR STOP???? OR BLOCK??? OR RESTRICT??? OR
               IMPED??? OR FREEZ??? OR FROZEN OR PAUS??? OR INTERRUPT?)
S5     414501   PIN OR PERSONAL()IDENTIFICATION()NUMBER? ? OR PASSWORD? ? -
               OR PASSCODE? ? OR PASSPHRASE? ? OR (PASS OR SECRET)()(WORD? ?
               OR CODE? ? OR PHRASE? ?) OR CREDENTIAL? ? OR AUTHENTICAT?
S6      72653   S5(7N)(ENTER??? OR ENTRY OR INPUT??? OR SUBMIT? OR TYPE? ?
               OR TYPING OR PROVID??? OR SUPPLY??? OR SUPPLIES OR SUPPLIED OR
                WRIT??? OR PRESENT???)
S7       3588   S5(7N)(SCREEN? ? OR BOX? ? OR PROMPT???)
S8         92   S4 AND S6:S7
S9         13   S8 AND AC=US/PR AND AY=(1963:2000)/PR
S10        22   S8 AND AC=US AND AY=1963:2000
S11        22   S8 AND AC=US AND AY=(1963:2000)/PR
S12        45   S8 AND PY=1963:2000
S13        51   S9:S12
S14        51   IDPAT (sorted in duplicate/non-duplicate order)
```

```
File 275:Gale Group Computer DB(TM) 1983-2006/Apr 03
         (c) 2006 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2006/Apr 03
         (c) 2006 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2006/Apr 03
         (c) 2006 The Gale Group
File  16:Gale Group PROMT(R) 1990-2006/Apr 04
         (c) 2006 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2006/Apr 03
         (c)2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Apr 03
         (c) 2006 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2006/Apr 03
         (c) 2006 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2006/Apr W4
         (c) 2006 CMP Media, LLC
File 674:Computer News Fulltext 1989-2006/Mar W4
         (c) 2006 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2006/Apr 03
         (c) 2006 Dialog
File 369:New Scientist 1994-2006/Aug W4
         (c) 2006 Reed Business Information Ltd.

Set     Items   Description
S1   10849027   PROGRAM? ? OR APPLICATION? ?
S2     507105   S1(5N)(RUN OR RUNNING OR EXECUT???)
S3     103488   S1(7N)(MEMORY OR RAM)
S4      11417   S2:S3(7N)(SUSPEND??? OR SUSPENSION OR DEFER??? OR DEFERMENT
              OR DELAY??? OR INHIBIT? OR HALT??? OR PREVENT??? OR DISABL? -
             OR HINDER??? OR STOP???? OR BLOCK??? OR RESTRICT??? OR IMPED?-
             ?? OR FREEZ??? OR FROZEN OR PAUS??? OR INTERRUPT?)
S5     770207   PIN OR PERSONAL()IDENTIFICATION()NUMBER? ? OR PASSWORD? ? -
             OR PASSCODE? ? OR PASSPHRASE? ? OR (PASS OR SECRET)()(WORD? ?
             OR CODE? ? OR PHRASE? ?) OR CREDENTIAL? ? OR AUTHENTICAT?
S6     143061   S5(7N)(ENTER??? OR ENTRY OR INPUT??? OR SUBMIT? OR TYPE? ?
             OR TYPING OR PROVID??? OR SUPPLY??? OR SUPPLIES OR SUPPLIED OR
              WRIT??? OR PRESENT???)
S7      13555   S5(7N)(SCREEN? ? OR BOX? ? OR PROMPT???)
S8         73   S4(50N)S6:S7
S9         49   RD  (unique items)
S10        39   S9 NOT PY=2001:2006
S11   8960930   RUN OR RUNNING OR EXECUT???
S12   1066114   MEMORY OR RAM
S13     23151   S1(7N)S11:S12(7N)(SUSPEND??? OR SUSPENSION OR DEFER??? OR -
           DEFERMENT OR DELAY??? OR INHIBIT? OR HALT??? OR PREVENT??? OR
           DISABL? OR HINDER??? OR STOP???? OR BLOCK??? OR RESTRICT??? OR
            IMPED??? OR FREEZ??? OR FROZEN OR PAUS??? OR INTERRUPT?)
S14       138   S13(50N)S6:S7
S15        97   RD  (unique items)
S16        42   S15 NOT (S10 OR PY=2001:2006)
S17   2248410   MODULE? ? OR ROUTINE? ? OR PROCESSES OR THREAD? ?
S18      5115   S17(7N)S11:S12(7N)(SUSPEND??? OR SUSPENSION OR DEFER??? OR
           DEFERMENT OR DELAY??? OR INHIBIT? OR HALT??? OR PREVENT??? OR
           DISABL? OR HINDER??? OR STOP???? OR BLOCK??? OR RESTRICT??? OR
            IMPED??? OR FREEZ??? OR FROZEN OR PAUS??? OR INTERRUPT?)
S19        15   S18(50N)S6:S7
S20        11   RD  (unique items)
```

WINDOWS NT® SERVER 4

SECURITY HANDBOOK



Lee Hadfield, Dave Hatter, Dave Bixler

QUE

Windows NT Server 4 Security Handbook

Library of Congress Catalog No.: 97-67039

ISBN: 0-7897-1213-x

99 98 97 6 5 4 3 2 1

Interpretation of the printing code: the rightmost double-digit number is the year of the book's printing; the rightmost single-digit number, the number of the book's printing. For example, a printing code of 97-1 shows that the first printing of the book occurred in 1997.

Screen reproductions in this book were created using Collage Plus from Inner Media, Inc., Hollis, NH.

Con

I

II

III

IV

V

The User Mode Security Components The User mode layer of the Windows NT operating system contains several components that work together to form the security subsystem. The security subsystem is comprised of the following components:

- *Log-on processes* These are the user mode processes that are used to authenticate users when they log on to the computer system. The log-on process is used to authenticate both local users and remote users.
- *Local Security Authority* This component is used in conjunction with the log-on process to verify that an individual has a legitimate user account on the system. This account status must be verified before access to the system is permitted. The Local Server Authority is the main component in the user mode portion of the security subsystem. Notice its user mode portion—there is one component of the security subsystem that is not a user mode component—the Security Reference Monitor. We'll explain more about that later in the chapter when we discuss the log-on and authentication process. The Local Security Authority is responsible for all interactive log-on activities and is the component that generates system access tokens *(SATs)*. It also is responsible for the audit control policy and the logging of audit messages generated by the Security Reference Monitor.
- *Security Account Manager (SAM)* This User mode component is responsible for maintaining the user accounts database that is used by the Local Security Authority to validate an individual's account during the log-on process.

These components combined with the Security Reference Monitor form the Windows NT Security Subsystem. This subsystem is not called an environmental subsystem, because it spans both the User mode and the Kernel mode. For this reason, it is called an *integral subsystem*. You learn more about how the Security Subsystem works later in the chapter when you see the log-on process and other object access issues.

Now, let's look at some of the changes that have been made to the operating system's architecture in Windows NT 4.0.

Learning the Architectural Changes in Windows NT 4.0

Windows NT 4.0 system architecture is based on the same architecture used with version 3.5 x, but with some modifications to both the Windows NT Executive and the Win32 subsystem. These modifications were made to improve system performance and still maintain the same degree of system integrity. (See Figure 3.4.)

device (video or printer) without knowing anything about the device. Consider this component to be the translator, taking the information from an application and then translating it into a language that the device drivers can understand.

- *Graphics Device Drivers* These are a set of DLLs that contain functions that allow the GDI to access the physical output devices. The most common output devices are monitors and printers. Device drivers take the translated information from the GDI and instruct the physical device to perform some type of action based on the translated information (or instructions). The use of drivers allows very specific device information to be implemented as separate and independent modules that can all hook into a common set of instructions. Some of these drivers are considered to be high-level drivers, others are considered to be the low-level drivers. The difference is the low-level drivers actually control hardware operation while high-level device drivers break the GDI calls into smaller pieces that the low-level drivers can understand.

Now that you've seen the individual components that comprise both the User mode and Kernel mode layers of the Windows NT operating system architecture, you can look at the various security processes that use these components.

Windows NT Security System Operation

User mode and Kernel mode layer components perform many of the internal system operations in Windows NT. Let's begin with a quick review of the components that make up the security subsystem. Here's a list of the components and their functions:

- *Log-on processes* These are the user mode processes that are used to authenticate users when they log on to the computer system.
- *Local Security Authority* This component is used in conjunction with the log-on process to verify that an individual has a legitimate user account on the system. This account status must be verified before access to the system is permitted. The Local Server Authority is the main component in the user mode portion of the security subsystem. The Local Security Authority is responsible for all interactive log-on activities and is the component that generates system access tokens (SATs). It is also responsible for the audit control policy and the logging of audit messages generated by the Security Reference Monitor.
- *Security Account Manager (SAM)* Now called the *directory services database*, this User mode component is responsible for maintaining the user accounts database that is used by the Local Security Authority to validate an individual's account during the log-on process.

The log-on process begins when a user presses the Ctrl+Alt+Del keys. This sequence of keystrokes is called the secure attention sequence, and it will always display the Windows NT operating system log-on screen. The intention here is to prevent the capture of a user's account name and password by a program that is imitating the Windows NT log-on screen (called a *Trojan Horse* program). This key sequence generates low-level function calls within the Windows NT operating system that can't be duplicated by application programs. However, it is possible to capture the Ctrl+Alt+Del keystrokes under DOS and redirect them. Therefore, it's possible that a DOS-based program running from a MS-DOS boot disk could simulate the Windows NT log-on screen and simply report some type of error while capturing the user's name and password. Again, the best prevention against this scenario is to always maintain tight physical security.

At this time the user must type in his or her account name and password in an interactive process that ultimately grants or denies access to the system. The user name and password gathered by the log-on process is then passed to the Local Security Authority that calls an authentication package.

The authentication package that is used may be custom written if necessary and does not necessarily have to have the authentication package that comes with Windows NT. This enables vendors to write custom packages that enable a user to log on to multiple systems at once, or use some sort of hardware-based device to authenticate users. Examples would be magnetic identification card scanners, voice recognition scanners, or even mechanical key devices.

The authentication package checks the account name and password against the names and passwords listed in the user accounts database. If a match is found the account is validated, the SAM returns the user's SID, and the security IDs of any groups the user belongs to. A log-on session is created by the authentication package. This log-on session along with all the SIDs are then passed back to the Local Security Authority.

At this time the SAT is created by the Local Security Authority. This token contains the SIDs of the user and any groups the user belongs to. In addition to the SIDs themselves, the SAT contains user rights information specific to each SID.

The token is then returned to the log-on process where it is attached to a process created by the Win32 subsystem on behalf of the user. This process, with its attached SAT, is called a *subject* for the user account. At this time the Win32 subsystem starts the desktop for an interactive user session.

If the authentication package cannot verify the user's account in the local accounts database, the information is forwarded to an alternative authentication package if one exists on the network. If the account validation fails, an error message is returned to the user notifying him or her that an incorrect account name or password has been entered. The user may then attempt to log on again.